Serial No. 09/884,672
Art Unit No. 2134

LISTING OF CLAIMS

1. (currently amended) An ad-hoc radio communication verification system, comprising:

means for sending data for verification data generation from ~~one~~ a first data send/receive device to a second ~~the other~~ send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first ~~one~~ data send/receive device, means for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to a first ~~its own~~ verification data output section;

in the second ~~other~~ data send/receive device, means for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to a second ~~its own~~ verification data output section; and

means for determining whether the verification data at the first and second verification data output sections ~~of both the data send/receive devices~~ matches mutually,

wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the first and second verification data output sections ~~of both the data send/receive devices~~ match mutually.

2. (original) The ad-hoc radio communication verification system according to claim 1, wherein the verification data is visual or auditory verification data.

3. (currently amended) The ad-hoc radio communication verification system according to claim 1, wherein the verification data is output at at least one of the first and second ~~the~~ verification data output sections ~~section~~ both in ~~the~~ visual form and auditory form.

4. (previously presented) The ad-hoc radio communication verification system according to claim 1, further comprising:

means for establishing a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way functions; and

means for letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

5. (canceled)

6. (currently amended) The ad-hoc radio communication verification system according to claim 1, further comprising:

means for establishing a serial sequence of operators that are composed of two or more of operators arranged in series, wherein the operators relate to the same or different one-way functions;

means for letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or

corresponding values be the verification data respectively; and

means for determining for each verification data whether the verification data match mutually at the first and second verification data output sections ~~of both the data send/receive devices~~.

7. (currently amended) The ad-hoc radio communication verification system according to claim 1, further comprising:

means for establishing a plurality of operators that relate to mutually different one-way functions;

means for letting the data for verification data generation be a common input to each operator and an output of each operator or a corresponding value be the verification data respectively; and

means for determining for each verification data whether the verification data match mutually at the first and second verification data output sections ~~of both the data send/receive devices~~.

8. (currently amended) The ad-hoc radio communication verification system according to claim 1, wherein the data

for verification data generation is a public key of one of said first and second ~~either~~ data send/receive devices ~~device~~.

9. (currently amended) An ad-hoc radio communication data send/receive system utilizing the ad-hoc radio communication verification system according to claim 8, comprising:

for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein each portable terminal comprises transmission means whereby a public key Kp of ~~one~~ a first user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of a second ~~the other~~ user without being tampered with, as determined by the ad-hoc radio communication system, and the public key Kp is transmitted from the portable terminal to the personal computer of each user, and wherein each personal computer comprises means to generate a symmetric key Kc such that the personal computer of the second ~~other~~ user generates a symmetric key Kc produced using a second generation algorithm, while the personal computer of the first ~~one~~ user

generates the symmetric key Kc produced using the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the second ~~other~~ user in cipher using the public key and deciphered at said personal computer of the first user; and thereafter both the personal computers send and receive data in cipher using the symmetric key Kc.

10. (currently amended) An ad-hoc radio communication data send/receive system utilizing the ad-hoc radio communication verification system according to claim 8, comprising, for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the ad-hoc radio communication verification system verifies that a public key Kp of the first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of the second ~~other~~ user without being tampered with, and wherein each personal computer comprises means to generate a symmetric key Kc such that the portable terminal

of the second ~~other~~ user generates a symmetric key Kc produced using a second generation algorithm, while the portable terminal of the first ~~one~~ user generates the symmetric key Kc produced using the second generation algorithm from information transmitted from the portable terminal of the second ~~other~~ user in cipher according to the public key and deciphered at the personal computer of the first user and transmits~~, then~~ the symmetric key Kc ~~is transmitted~~ from the portable terminal to the personal computer of each user; and thereafter both the personal computers send and receive data in cipher using the symmetric key Kc.

11. (currently amended) An ad-hoc radio communication data send/receive system, comprising, for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp of a first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of

the second ~~other~~ user without being tampered with, the public key Kp is transmitted from the portable terminal to the personal computer of each user, and wherein each personal computer comprises means to generate a symmetric key Kc such that the personal computer of the second ~~other~~ user generates a symmetric key Kc produced using a second generation algorithm, while the personal computer of the first ~~one~~ user generates the symmetric key Kc produced using the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the ~~other~~ second user in cipher according to the public key and deciphered by the personal computer of the first user; and thereafter both the personal computers send and receive data in cipher using the symmetric key Kc.

12. (currently amended) An ad-hoc radio communication data send/receive system, comprising, for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp

of a first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of ~~the other~~ a second user without being tampered with, and wherein each personal computer comprises means to generate a symmetric key Kc such that the portable terminal of the ~~other~~ second user generates a symmetric key Kc produced using a second generation algorithm, while the portable terminal of the first ~~one~~ user generates the symmetric key Kc produced using the second generation algorithm from information transmitted from the portable terminal of the ~~other~~ second user in cipher according to the public key and deciphered by the portable terminal of the first user, and transmits ~~then~~ the symmetric key Kc ~~is transmitted~~ from the portable terminal to the personal computer of each user; thereafter both the personal computers send and receive data in cipher using the symmetric key Kc.

13. (currently amended) A method for verifying an ad-hoc radio communication, comprising the steps of:

sending data for verification data generation from a first ~~one~~ data send/receive device to a second ~~the other~~ send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first ~~one~~ data send/receive device, generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to a first ~~its own~~ verification data output section;

in the second ~~other~~ data send/receive device, generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to ~~its own~~ a second verification data output section; and

determining whether the verification data at the first and second verification data output sections ~~of both the data sections of both the data send/receive devices matches~~ match mutually,

~~wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually~~.

14. (original) The method according to claim 13, wherein the verification data is visual or auditory verification data.

15. (currently amended) The method according to claim 13, wherein the verification data is output at at least one of the first and second ~~the~~ verification data output sections ~~section~~ both in the visual form and auditory form.

16. (previously presented) The method according to claim 13, further comprising the steps of:

establishing a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way functions;

letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

17. (canceled)

18. (previously presented) The method according to claim 13, further comprising the steps of:

establishing a serial sequence of operators that are composed of two or more of operators arranged in series wherein the operators relate to the same or different one-way functions;

letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively; and

determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

19. (previously presented) The method according to claim 13, further comprising the steps of:

establishing a plurality of operators that relate to mutually different one-way functions;

letting the data for verification data generation be a common input to each operator and an output of each operator or a corresponding value be the verification data respectively; and

determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

20. (currently amended) The method according to claim 13, wherein the data for verification data generation is a public key of one of said first and said second ~~either~~ data send/receive ~~device~~ devices.

21. (currently amended) The method for sending and receiving ad-hoc radio communication data, utilizing the verification method according to claim 20, ~~comprising:~~ wherein each user has a portable terminal having a radio communication function for said each user and a personal computer having a radio communication function for the each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein the method further comprises, when the verification method verifies that a public key Kp of the first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of the second ~~other~~ user without being tampered with, transmitting the public key Kp ~~is transmitted~~ from the portable terminal to the personal

computer of each user; ~~, then~~ the personal computer of the ~~other~~ second user generating ~~generates~~ a symmetric key Kc produced using a second generation algorithm; ~~, while~~ the personal computer of the first ~~one~~ user generating ~~generates~~ the symmetric key Kc produced using the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the second ~~other~~ user in cipher according to the public key and deciphered by the personal computer of said first user; and ~~thereafter~~ both the personal computers sending and receiving ~~send and receive~~ data in cipher using the symmetric key Kc.

22. (currently amended) The method for sending and receiving ~~and receiving~~ ad-hoc radio communication data, utilizing the verification method according to claim 20, ~~comprising:~~ wherein each user has a portable terminal having a radio communication function for each user and a personal computer having a radio communication function for each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein said method further comprises, when the verification method verifies that a public key Kp of the first ~~one~~ user is

transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of the second ~~other~~ user without being tampered with, the portable terminal of the second ~~other~~ user generating ~~generates~~ a symmetric key Kc produced using a second generation algorithm; ~~, while~~ the portable terminal of the first ~~one~~ user generating ~~generates~~ the symmetric key Kc produced using the second generation algorithm from information transmitted from the portable terminal of the second ~~other~~ user in cipher according to the public key and deciphered by the portable terminal of the first user; and transmitting ~~, then~~ the symmetric key Kc ~~is transmitted~~ from the portable terminal to the personal computer of each user; and ~~thereafter~~ both the personal computers sending and receiving ~~send and receive~~ data in cipher using symmetric key Kc.

23. (currently amended) The method for sending and receiving ad-hoc radio communication data, ~~comprising:~~ wherein each user has a portable terminal having a radio communication function for each user and a personal computer having a radio communication function for each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein said

method further comprises, when it is verified that a public key Kp of the first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of the second ~~other~~ user without being tampered with, transmitting the public key Kp ~~is transmitted~~ from the portable terminal to the personal computer of each user; ~~, then~~ the personal computer of the second ~~other~~ user ~~generates~~ generating a symmetric key Kc produced using a second generation algorithm; ~~, while~~ the personal computer of the first ~~one~~ user generating ~~generates~~ the symmetric key Kc produced using the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the second ~~other~~ user in cipher according to the public key and deciphered by the personal computer of the first user; and thereafter both the personal computers sending and receiving ~~send and receive~~ data, in cipher using the symmetric key Kc.

24. (currently amended) The method for sending and receiving ad-hoc radio communication data, wherein each user has ~~comprising:~~ a portable terminal having a radio communication function for each user and a personal computer having a

radio communication function for each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein said method further comprises, when it is verified that a public key Kp of the first ~~one~~ user is transmitted from the portable terminal of the first ~~one~~ user to the portable terminal of the second ~~other~~ user without being tampered with, the portable terminal of the second ~~other~~ user ~~generates~~ generating a symmetric key Kc produced using a second generation algorithm; ~~, while~~ the portable terminal of the first ~~one~~ generating ~~generates~~ the symmetric key Kc produced using the second generation algorithm from information transmitted from the portable terminal of the ~~other~~ second user in cipher according to the public key and deciphered by the portable terminal of the first user; transmitting~~, then~~ the symmetric key Kc ~~is transmitted~~ from the portable terminal to the personal computer of each user; and, thereafter both the personal computers ~~send and receive~~ sending and receiving data in cipher using the symmetric key Kc.

25. (currently amended) A recording medium recording a program for an ad-hoc radio communication verification system, wherein the verification system comprising:

means for sending data for verification data generation from a first ~~one~~ data send/receive device to ~~the other~~ a second send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first ~~one~~ data send/receive device, means for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to a first ~~its own~~ verification data output section;

in the second ~~other~~ data send/receive device, means for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to a second ~~its own~~ verification data output section; and

means for determining whether the verification data at the verification data output sections of ~~both~~ the first and second data send/receive devices matches mutually,

wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the first and second verification data output sections ~~of both the data send/receive devices~~ match mutually.

26. (original) The recording medium according to claim 25, wherein the verification data is visual or auditory verification data.

27. (currently amended) The recording medium according to claim 25, wherein the verification data is output at at least one of the first and second ~~the~~ verification data output ~~section~~ sections both in the visual form and auditory form.

28. (currently amended) The recording medium according to claim 25, wherein the verification system further comprises ~~comprising~~:

means for establishing a serial sequence of operators that are composed of more than one operators arranged in

series, wherein the operators relate to the same or different one-way functions; and

means for letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

29. (canceled)

30. (currently amended) A delivery system for delivering a program for an ad-hoc radio communication system, the verification system comprising:

means for sending data for verification data generation from a first ~~one~~ data send/receive device to a second ~~the other~~ send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first ~~one~~ data send/receive device, means for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to a first ~~its own~~ verification data output section;

in the second ~~other~~ data send/receive device, means for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to a second ~~its own~~ verification data output section; and

means for determining whether the verification data at the first and second verification data output sections ~~of both the data send/receive devices matches~~ match mutually,

wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the first and second verification data output sections ~~of both the data send/receive devices~~ match mutually.

31. (previously presented) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1.

32. (previously presented) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 4.

33. (previously presented) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 9.

34. (previously presented) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable

program code means for causing a computer to effect the functions of claim 10.

35. (original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 11.

36. (canceled)

37. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

38. (original) An article of manufacture comprising a computer usable medium having computer readable program code

means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 21.

39. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

40. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 23.

41. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 24.

42. (canceled)

43. (canceled)